

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

IN THE MATTER OF THE SEARCH OF INFORMATION )  
ASSOCIATED WITH THE GOOGLE ACCOUNTS )  
RICHARDDMILLER1984@GMAIL.COM AND )  
PAMELASARGENT493@GMAIL.COM, THAT IS STORED )  
AT PREMISES CONTROLLED BY GOOGLE LLC AND )  
GOOGLE PAYMENT CORPORATION )

FILED UNDER SEAL

4:24 MJ 9306 RHH

SIGNED AND SUBMITTED TO THE COURT  
FOR FILING BY RELIABLE ELECTRONIC  
MEANS

## APPLICATION FOR A SEARCH WARRANT

I, Prestyn Atherton, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the \_\_\_\_\_ District of California, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

18 U.S.C. § 2251 (production of child pornography), and 2252A(a)(1) & (2) (distribution of child pornography)

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct

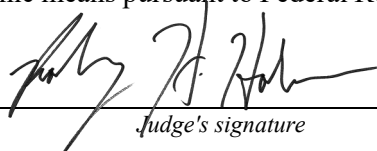
  
\_\_\_\_\_  
Applicant's signature

Prestyn Atherton, SA, HSI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: Jul y 23, 2024

  
\_\_\_\_\_  
Judge's signature

City and State: St. Louis, Missouri

Honorable Rodney H. Holmes, U.S. Magistrate Judge

Printed name and title

AUSA: JILLIAN ANDERSON

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
GOOGLE ACCOUNTS  
**RICHARDDMILLER1984@GMAIL.COM**  
AND  
**PAMELASARGENT493@GMAIL.COM**,  
THAT IS STORED AT PREMISES  
CONTROLLED BY GOOGLE LLC AND  
GOOGLE PAYMENT CORPORATION

**FILED UNDER SEAL**

4:24 MJ 9306 RHH

SIGNED AND SUBMITTED TO THE  
COURT FOR FILING BY RELIABLE  
ELECTRONIC MEANS

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Prestyn Atherton, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since

July 2023. I am currently assigned to the HSI office in Saint Louis, Missouri. In that role, I investigate a variety of different federal criminal violations, including federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I completed training on these and related topics through the Federal Law Enforcement Training Center (FLETC), Criminal Investigator Training Program (CITP), Homeland Security Investigations Special Agent Training (HSISAT), and through various in-service trainings offered through my agency and external partners. This training includes the requirement to observe, review, and classify numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in several forms of electronic media. I hold a bachelor's degree with a dual major in Criminal Justice and Management. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from personal observations, training and experience, and information obtained from other law enforcement and witnesses. This affidavit is merely intended to show sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (production of child pornography), and 2252A(a)(1) & (2) (distribution of child pornography) were committed by Richard James MILLER. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and contraband of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

### **LOCATION TO BE SEARCHED**

7. The location to be searched is:

Google Account: **richarddmiller1984@gmail.com** and **pamelasargent493@gmail.com**, located at a premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

### **BACKGROUND CONCERNING GOOGLE**<sup>1</sup>

8. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site

---

<sup>1</sup> The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at [lers.google.com](https://lers.google.com); product pages on [support.google.com](https://support.google.com); or product pages on [about.google.com](https://about.google.com).

called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

9. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

10. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

11. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

a. Gmail - Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google.

b. Contacts - Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list

called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account, so it is stored in Google Contacts. Google preserves contacts indefinitely unless the user deletes them.

c. Calendar - Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

d. Messaging - Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

e. Google Drive and Keep - Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form

service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely unless the user deletes them.

f. Photos - Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely unless the user deletes them.

g. Maps - Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an

itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely unless the user deletes it.

h. Location history - Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.



i. Google Pay and records of payments for Google services - A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

j. Chrome and My Activity - Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio

Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

k. Google Voice - Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely unless the user deletes them.

l. YouTube - Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

12. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

13. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

14. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of

service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

15. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

16. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, by comparing Google service login history, with location history, to the dates and times other applications were used, or media files were created or accessed shows a specific user is likely attributed to that activity.

17. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

18. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing

a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

19. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

20. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

**PROBABLE CAUSE**

21. On March 18, 2024, Homeland Security Investigations (HSI) Cherry Hill, New Jersey executed a search warrant in furtherance of a child exploitation investigation. Your undersigned affiant was briefed about this investigation, including the information set forth below.

22. Upon forensic review of a phone seized during the search warrant, a Kik messenger group chat was identified between the subject of the investigation and two unknown Kik users, “MasterDogg69” and a third user unrelated to this application. The context of the group chat was for like-minded individuals to discuss sexual abuse of family members, including children. In the group chat, “MasterDogg69” shared explicit photographs of girls he claimed were his teenage daughters. The user of the Kik Messenger account “MasterDogg69” states in the chat that he is from Missouri and the abuse began when the children were about 10 years old.

23. On April 10, 2024, HSI Cherry Hill contacted HSI St. Louis regarding Kik user “Masterdogg69” and suspected criminal activity that occurred within the HSI St. Louis Area of Responsibility (AOR), and an investigative referral was sent on April 23, 2024.

**Subpoena for Kik Account User “MasterDogg69”:**

24. Your undersigned affiant was further informed as follows regarding subpoenas sent to Kik Messenger and Charter Communications by HSI Cherry Hill. On March 27, 2024, HSI Cherry Hill agents sent a DHS summons to Kik c/o MediaLab.ai Inc. regarding username “MasterDogg69” requesting Internet Protocol (IP) addresses and subscriber data associated with the account. On March 28, 2024, Kik provided the following, as well as other, subscriber information and IP address for the user:

Username: Masterdogg69

First name: M. Crazy

Last Name: Dogg69

Email: lovedoctor1984@yahoo.com (confirmed)

Kik provided the following IP address associated with the account for the timeframe of February 28, 2024 – March 26, 2024: 75.133.153.127

**Subpoena for Charter Communications for IP 75.133.153.127:**

25. On April 4, 2024, HSI Cherry Hill agents sent a DHS summons to Charter Communications, Inc. (hereinafter, “Charter”) for subscriber information and log data for IP address 75.133.153.127 for March 4, 2024, during the time the Kik account “MasterDogg69” was actively sending messages and images on the group chat. Charter provided subscriber information and log data for the timeframe of February 28, 2024-March 26, 2024, for that IP address which showed service address: 1100 N SAINT JOE DR, APT 21, PARK HILLS, MO 63601-1944.

**Identification of Richard MILLER**

26. Government and commercial databases link 1100 North Saint Joe Drive, Unit 21, Park Hills, Missouri 63601 (hereinafter “MILLER’S RESIDENCE”) to Richard James MILLER (DOB: 10/04/1984). A U.S. Department of Housing and Urban Development (HUD) Office of Inspector General (OIG) Special Agent (SA) confirmed that MILLER received HUD assistance at that address, a single bedroom apartment located within the St. Francis Heights Apartments complex. Missouri Department of Revenue records show MILLER’s RESIDENCE on his State Identification card.

**Review of Kik Group Chat:**

27. Your undersigned affiant reviewed the Kik group chat digital evidence discovered by HSI Cherry Hill during the execution of a search warrant in their investigation, wherein I

observed Kik user “Masterdogg69” in a chat with two other users, discussing incestual fantasies and sharing stories of incest/sexual abuse. Kik user “MasterDogg69” distributed multiple image files that appear to depict pubescent females engaged in sexually explicit conduct, which “MasterDogg69” stated were his 18 and 16-year-old daughters. “MasterDogg69” stated that he began sexually abusing the girls when they were 10 years old. The following is a summation of content I observed in the chat. All the messages summarized below were sent on March 4, 2024, between 1:47 PM and 8:19 PM.

28. “MasterDogg69” stated that he was from Missouri.

29. “MasterDogg69” stated that he regularly engages in sexual intercourse with who he claimed is his then 16-year-old and 18-year-old daughters. “MasterDogg69” stated that he believed his daughters were 10 years of age when he started sexually abusing them.

30. “MasterDogg69” stated, “My other will be 17 tomorrow, which is legal in my state” referring to his youngest daughter and offered to send pictures of her to the other users in the chat.

31. “MasterDogg69” distributed several image files that depicted what appears to be a pubescent female, which the user claimed was his 16-year-old daughter, completely nude with lascivious display of her genitals and engaged in masturbation. One image depicts the nude lower half of a female’s body sitting in a bathtub. Two other images depict what appear to be a video thumbnail of the nude lower half of a female engaged in masturbation in a bathtub. In another image file sent, a fully nude female is standing in front of a mirror taking a selfie. Her face and genitals are visible.

32. “MasterDogg69” sent an image file of what appears to be a video thumbnail of a female, which he claimed to be his 16-year-old daughter, engaged in sex with a male and stated, “This me and her fucking in her pussy.”



33. Another user in the chat stated that it looks like “MasterDogg69” has consensual and non-consensual sex whenever he wants with the females and “MasterDogg69” responded, “Exactly.” “MasterDogg69” later stated “I get what I want when I want mainly they love it that way.”

34. “MasterDogg69” distributed image files depicting what appears to be a pubescent female engaged in sexually explicit conduct, which he stated was his now 18-year-old daughter. In one image, there is a man engaged in what appears to be oral sex on a female and half of the man’s face is visible. The hair, facial hair, and other facial features of the man are generally consistent with the individual depicted in the photograph on Richard MILLER’s Missouri state identification card and the adult male your undersigned affiant saw enter MILLER’S RESIDENCE while conducting surveillance on May 3, 2024. In the background of 2 images, a dark stained wood door can be seen that appears to be the same door in the background of other pictures sent by “MasterDogg69”.

35. “MasterDogg69” sent two other image files of females engaged in sexually explicit conduct with a man and claimed they were of his “other oldest” and his sister. Half of the man’s face is visible, and his facial hair and other facial features are generally consistent with that of a man your undersigned affiant observed enter the MILLER’S RESIDENCE while conducting surveillance on May 3, 2024, and the individual depicted in the photograph on Richard MILLER’s Missouri state identification card. In the background of the image, a dark stained wood door can be seen that appears to be the same door in the background of other pictures sent by “MasterDogg69”.

**Execution of Search Warrant at MILLER'S RESIDENCE**

36. On May 24, 2024, your undersigned affiant applied for and received federal criminal search and seizure warrant No. 4:24 MJ 6106 PLC from the United States District Court for the Eastern District of Missouri for MILLER'S RESIDENCE. On June 4, 2024, HSI Special Agents and local law enforcement executed the search and seized two (2) laptop computers and three (3) cellular phones and took photos of the interior of the apartment which matched those in the background of the child exploitation images distributed by MILLER on Kik. In particular, the above-mentioned dark wood-stained door and white closet door in the bedroom of MILLER's apartment, as well as what can be described as Native American artifacts hanging on the wall, all of which can be seen in the background of photos sent by MILLER in the Kik chat.

**Interview of MILLER**

37. Concurrent with execution of the residential search warrant Special Agents interviewed MILLER. In a post warned statement MILLER admitted he used the Kik application under username mistercrazywolf or mcrazywolf69 and, after being shown chat transcripts, also confirmed he may have used the username MasterDogg69. MILLER stated he thought his Google account was whitedogg69@gmail.com and later stated it may be whitedogg1956@gmail.com. MILLER confirmed that there should be three (3) cellular phones in his apartment, two (2) of which (described as a Samsung and Vortex Phone) belong to him and one (1) of which (described as a blue TracFone) belongs to a minor victim with initials LR (hereinafter referred to as "MV1"). MILLER confirmed there should be two (2) laptop computers (described as HP and Lenovo) which belong to him. All five (5) devices were found in the residence and seized as evidence.

38. MILLER admitted to receiving and accidentally clicking on a link to download child pornography on Kik the day prior, June 3, 2024, using account username mcrazywolf69.

39. MILLER admitted to engaging in sexual intercourse and oral sex with MV1, recording/photographing it, and then distributing the explicit images of her to other users on Kik messenger. MILLER stated he distributed the images as recently as the evening of June 3, 2024. MILLER confirmed that he has knowledge that MV1 is 17 years of age and stated he thought she was 17 years of age at the time the videos/photos were taken. MILLER was shown a transcript of the above described Kik chat and confirmed that he was the author of the chat, was using Kik username MasterDogg69, and that some of the images/videos he distributed were videos he produced of himself and MV1 nude and engaged in sexual intercourse. MILLER stated that he refers to MV1 as his “daughter,” although they are not related. MILLER stated that he has known and spent time with MV1 for 3 years.

40. MILLER admitted to engaging in sexual intercourse with a second female with the initials KS (hereinafter “KS”), whom he stated he thought was 19 years of age, recording/photographing it, and then distributing the explicit images of her to other users on Kik. MILLER was shown the portion of the above mentioned Kik chat transcript and confirmed that KS is one of the females depicted in the images on the chat engaged in oral sex, sexual intercourse, and lascivious display of the genitals and that he produced the images. MILLER stated he thought she was 18 years of age at the time of the chat. MILLER stated that he would refer to her as his “daughter” even though they are of no relation.

41. Upon review of the rest of the explicit images distributed in the Kik chat, MILLER stated that the other females depicted in the images were of a mother and daughter from another

state who came to visit and have sex “a while ago.” He claimed that the daughter is going to be graduating high school this year. He later denied having sex with them and stated that the mother sent him the images.

**Interview of Minor Victim One (1)**

42. On June 6, 2024, a HSI Forensic Interview Specialist (FIS) interviewed a minor victim associated with this case with the initials LR (hereinafter referred to as “MV1”). MV1 stated she is 17 years of age and that she was 15 years of age when she first met MILLER and began spending time at his apartment. MV1 stated she engaged in oral sex and sexual intercourse with MILLER on multiple occasions starting when she was 15 years of age. MV1 stated he would use sex toys described as a vibrator, dildo, handcuffs, ball and chain, collar with leash, and strawberry flavored lube on her and two other juvenile females. MV1 stated that MILLER would sometimes force her and two other juvenile females, one of which she thought to be 9 years of age and the other 17 years of age at the time of the abuse, to have sex or engage in oral sex with him. MV1 stated that MILLER would use his cell phone to photograph and record her, and the other juveniles, fully nude and while engaging in sexually explicit conduct. MV1 stated MILLER would manipulate or force her to send him photographs and videos of her nude and engaged in masturbation and threatened to hurt MV1’s dad if she told anyone or stopped. MV1 state that MILLER would distribute the pornographic photographs and videos of her to other users on Kik Messenger and would show her the chat and the other users’ responses to the images. MV1 stated that MILLER would often refer to her as his “daughter.” MV1 was shown pictures of the above-described explicit images sent on Kik by MasterDogg69 described as “Pictures 1-6”. MV1 confirmed that the images were of her when she was 16 years of age and that the username used

to distribute them (MasterDogg69) was a username she recognized as one used by MILLER on Kik. It should be noted that MV1 confirmed that one of the video thumbnails described above, which MILLER stated in the chat was him engaging in sex with his 16-year-old daughter and labeled in this interview as “Picture 4,” was a video of MV1 and MILLER engaged in sexual intercourse. MV1 stated she also observed MILLER use a username which she thought to be mcrazywolf69 to distribute images/videos of her on Kik. MV1 also stated that she would send explicit images to MILLER via Snapchat username whitedogg1956, display name “White Dogg69” and MILLER would send explicit images of himself to her.

### **Interview of Victim Two (2)**

43. On June 6, 2024, the FIS interviewed a victim associated with this case, described above by MV1 as the 17-year-old juvenile female, with the initials KS (hereinafter referred to as “KS”). KS stated she is 19 years of age and that she was 17 years of age when she first met MILLER and began spending time at his apartment. KS stated that she engaged in sexual intercourse and oral sex with MILLER multiple times starting when she was 17 years of age. KS stated she witnessed MV1 and MILLER have sexual intercourse and oral sex when MV1 was 15 years of age. KS stated that MILLER recorded both MV1 and herself engaged in sexually explicit conduct and distributed the images to other users on Kik. KS stated that MILLER would request sexually explicit videos/photographs of her genitals and engaged in masturbation and would then distribute those videos to other users on Kik and show her the chat. KS was shown the explicit images suspected to be of her distributed by MILLER in the above-mentioned chat and she confirmed that it was her and MILLER depicted in the images. KS stated that she would also send explicit images of herself to MILLER’s snapchat username whitedogg1956. KS stated that

MILLER showed her a video on his cell phone of a “little boy,” whom she thought to be a young child, having sex with a grandma. KS stated that MILLER had multiple phones. KS stated that MILLER would use the above-mentioned sex toys on both her and MV1.

### **Interview of Minor Victim Three (3)**

44. On June 6, 2024, the FIS interviewed a minor victim associated with this case, identified as one of the female juveniles described above by MV1, with the initials KS (hereinafter referred to as “MV3”). MV3 stated she is 10 years of age and that she first met MILLER and began spending time at his apartment approximately 2 years ago. MV3 stated that her dad and MILLER were good friends and that their family stayed at MILLER’s apartment for a period of time when they were homeless. MV3 stated that MILLER and MV1 had sex in front of her. MV3 stated that MILLER touched her thighs inappropriately and showed her pornographic videos, including that of bestiality. MV3 stated she saw MILLER and MV1 use the above-mentioned sex toys in front of her. MV3 stated she knew MILLER recorded/photographed MV1 and KS engaged in sexually explicit conduct and sent the images on the internet. MV3 stated she was not comfortable stating anymore because she was afraid her mother would be mad at her.

### **Review of Devices Seized During Search Warrant**

45. As a result of the search warrant executed on June 4, 2024, three (3) cellular phones and two (2) laptops were seized from MILLER’s residence. Forensic examination of the devices seized from the residence is ongoing, but I observed artifacts of Kik usernames Masterdogg69 and mcrazywolf69 and Google account whitedogg1956@gmail.com suggesting use by and attribution to MILLER across multiple devices seized from the residence.

46. A manual and forensic review of the device described as a Vortex HD65 Plus Android Cell phone, IMEI 359525842487038 (hereinafter “Vortex Phone”), which MILLER stated was his device, provided the correct passcode for, and gave a matching phone number for, revealed the presence of Child Sexual Abuse Material (CSAM). Explicit photographs of the above-identified MV1, KS, and MV3 engaged in lascivious display of the genitals, sexual intercourse and masturbation were found on the device, including the above-described images sent in the Kik chat. There are multiple images of MV3 engaged in lascivious display of the genitals and sexual intercourse in what appears to be MILLER’s apartment bedroom. The same room décor, painting, dark wood-stained doors, and white closet door, which is in MILLER’s apartment bedroom can be seen in the background of the explicit images of MV3. Numerous other explicit videos and photos of age-difficult, unidentified females were also found on the device.

47. The Vortex Phone was logged into and linked to automatically sync and backup to Google account: whitedogg1956@gmail.com. Sexually explicit video thumbnails can be seen stored in the Google account, but since the forensic and manual review of the device is done in “airplane mode” (not connected to the internet), the videos will not play and a search warrant for the Google account was needed to further access that data. On June 21, 2024, search warrant No. 4:24 MJ 3211 NCC was signed and executed on Google for account information pertaining to whitedogg1956@gmail.com.

### **The Subject Google Accounts**

48. On June 26, 2024, Google LLC provided responsive records for account whitedogg1956@gmail.com under Google Reference Number 63140615. Review of that material is ongoing, but revealed artifacts indicating distribution or receipt of child pornography between

whitedogg1956@gmail.com and SUBJECT ACCOUNTS richarddmiller1984@gmail.com and pamelasargent493@gmail.com. For example:

49. On March 17, 2024, richarddmiller1984@gmail.com received two (2) child pornography videos depicting MV1 engaged in masturbation from whitedogg1956@gmail.com.

a. MD5 Hash: 3e826d6d447a3c90e77ee4a62d2387684f282, file name: received\_386637584315179.mp4 and email subject line: “[MV1’s first name] and me.”

b. MD5 Hash: 9e6264121154d1501a41ca6de26b501f, File name: received\_944452583933440, and email subject: “[MV1’s first name] and me.”

50. Further attribution to MILLER’s ownership of the account richarddmiller1984@gmail.com is the name and numbers matching that of Richard MILLER and his year of birth, 1984.

51. On March 13, 2023, account pamelasargent493@gmail.com sent an email with attachment to whitedogg1956@gmail.com containing a child pornography video file of what appears to be two (2) toddler-aged minor male victims fully nude in the bath. Depicted in the video, one of the minor victims places his penis on the back/buttocks of the other minor victim and later in the video, one of the minor victims sits on the penis of the other minor victim. A woman’s voice, who is presumably filming the children, can be heard in the background instructing one of the children to, “sit on bubby” and “go up and down.” The following are the identifiers of the video image file containing child pornography:



- a. MD5 Hash: d7405ab4cd11f274193e79470dd92457, File Name: IMG\_8363.MOV,  
Email subject line: None.

52. On March 13, 2023, account pamelasargent493@gmail.com sent an attachment to whitedogg1956@gmail.com containing a child pornography video image file of what appears to be two toddler-aged minor male victims fully nude in the bath. Depicted in the video, one of the minor victims places his mouth on the penis and anus of the other minor victim. The following are the identifiers of the video image file containing child pornography:

- a. MD5 Hash: 82252b27e07ca9437cd5e3487e87c4d8, File Name: IMG\_8362.MOV,  
Email subject line: None.

53. On September 6, 2023, account pamelasargent493@gmail.com received an email with attachment from whitedogg1956@gmail.com containing a child pornography video file of the above-identified MV3 engaged in sexual intercourse with an adult male. Depicted in the video, MV3 is fully nude and straddling a nude adult male in a position and with movements consistent with that of sexual intercourse. The adult male depicted in the video resembles the likeness of MILLER and the incident was filmed in an apartment bedroom matching the description of a bedroom in MILLER's RESIDENCE. The voice of the adult male can be heard in the audio of the video, and it resembles the voice of MILLER. The following are the identifiers of the video image file containing child pornography:

- a. MD5 Hash: a791e1fec4540c30b71d88f118707c8e, File Name: Video.MOV, Email  
subject line: "My niece I mean."

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

54. Your undersigned affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**CONCLUSION**

55. Based on the forgoing, your undersigned affiant request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

57. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

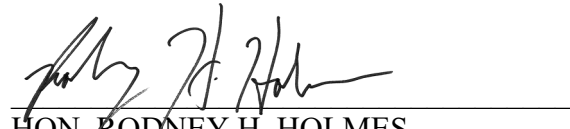
destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



Prestyn Atherton  
Special Agent  
Homeland Security Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 23rd day of July, 2024.



HON. RODNEY H. HOLMES  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**4:24 MJ 9306 RHH**

**Property to Be Searched**

This warrant applies to information associated with **richarddmiller1984@gmail.com** and **pamelasargent493@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC and Google Payment Corporation a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**4:24 MJ 9306 RHH**

**Particular Things to be Seized**

**I. Information to be disclosed by Google LLC and Google Payment Corporation (“Google”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 30, 2024 with Google Reference Number 63748160, and July 12, 2024 Google Reference Number 64678710, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from March 1, 2019 to present, unless otherwise indicated:

- a. All business records and subscriber information, in any form kept, pertaining to the Account, including:
  1. Names (including subscriber names, user names, and screen names);
  2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
  3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
  4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
  5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
  6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and
  8. Change history.
- b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
  - c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs
  - d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.
  - e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.
  - f. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history.
  - g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
  - h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously

accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

- i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
- j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.
- k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.
- l. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history.
- m. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.
- n. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including

deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

- o. All records, content, and other information relating to YouTube use and access, including, but not limited to, associated videos (including records of uploads, shares, views, edits, comments, likes, and other interaction; and copies of videos uploaded to, shared by, or shared with the account), searches (including search terms), channels, subscriptions and subscribers, playlists, connected apps, user settings, friends and other contacts (including the content of all communications), deletions and other changes, and, for videos, URL, metadata, privacy and other settings, size, title, description, duration, tags, timestamps, IP addresses, location information, and the account or other identifier of the user who uploaded the video; video and channel performance information, including all analytics on content, reach, engagement, audience, revenue, and research; and, for all of the above, all related logs, IP addresses, timestamps, and device identifiers.

**Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.**

## **II. Information to be seized by the United States**

All information described above in Section I that constitutes contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) and (a)(5)(B), those violations involving Richard James MILLER and occurring from March 1, 2019, to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The purchase, receipt, or possession of child pornography or attempts to commit, including any such contraband material stored within Google Drive or as attachments to messages, even when deleted or marked for deletion;
- b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).



- e. The identity of the person(s) who communicated with the Account about matters relating to receipt and distribution of child pornography, including records that help reveal their whereabouts.